

**IN THE UNITED STATES DISTRICT COURT
SOUTHERN DISTRICT OF NEW YORK**

THE NIELSEN COMPANY (US), LLC,

Plaintiff,

v.

TVSQUARED LTD.,

Defendant.

Civil Action No. 23-CV-1581 (VSB)

JURY TRIAL DEMANDED

DECLARATION OF PAUL D. MARTIN, PH.D.

I, Paul D. Martin, Ph.D., declare as follows:

INTRODUCTION AND ENGAGEMENT

1. I have been retained on behalf of The Nielsen Company (US), LLC (“Nielsen”) to offer technical opinions relating to U.S. Patent No. 10,063,378 (“the ’378 Patent”).

2. I have no financial interest in either party to, or in the outcome of, the above-styled proceeding. I am being compensated for my work as an expert on an hourly basis at my standard consulting rate. My compensation is not dependent on the outcome of these proceedings or the content of my opinions.

PERSON OF ORDINARY SKILL IN THE ART

3. In my opinion, a person of ordinary skill in the art (“POSA”) in the field of the ’378 Patent would have a working knowledge of the software and/or hardware of systems that retrieve and associate user information while protecting user privacy. The POSA would have gained this knowledge through an undergraduate degree in an applicable engineering field (for example, electrical or computer engineering or computer science) and at least two years of work experience in relevant fields.

MY EXPERTISE

4. My CV, attached to this declaration as Exhibit A, demonstrates my expertise in the field of the '378 Patent.

5. I hold B.S., M.S.E., and Ph.D. degrees in computer science from Johns Hopkins University and have worked in the areas of software engineering, privacy, cybersecurity, and applied cryptography for more than 10 years. In my professional work, I have led a wide variety of security and privacy projects, including developing vulnerability assessment applications, performance testing, cryptographic protocol design and implementation, and development of systems that retrieve and associate user information while protecting user privacy.

6. I have published research on systems security and applied cryptography, including foci on low-overhead and super-scalable security solutions as well as on cryptographically secure authentication protocols. My work has led to the development of commercial products and services, such as a Hadoop-based application for large-scale statistical analysis of audit logs and a web-based traffic visualization dashboard for smart grid networks. I am a named inventor on several patents in these areas.

7. At Harbor Labs, I manage client engagements and lead teams focused on security and cryptographic analysis and source code analysis. I have reviewed software systems of varying sizes across numerous industries, including security, cryptography, television-based set-top boxes, network appliances, web-based enterprise systems, email management systems, telephony products, embedded system bootloaders, and social network platforms.

8. I also serve as the technical and development lead for a firmware security analysis product called Firmware IQ. This product is designed to analyze the firmware of embedded devices for security and cryptographic vulnerabilities in an automated fashion. In one configuration of the product, a developer uploads a firmware image to a web-based portal, which uses a broker to

forward the firmware to an engine for analysis. The engine unpacks the firmware, breaks it into its constituent components, and performs more than one hundred automated security and cryptography checks to find vulnerabilities in the firmware image.

INFORMATION RELIED UPON

9. In formulating my opinions, I have relied upon the '378 Patent as well as other materials referenced in Appendix A to this declaration. I have also relied upon my education and work experience. Counsel has informed me that I should look through the lens of one skilled in the art of the field of the '378 Patent at the time of the priority date of the '378 Patent, and I have done so. I have assumed the priority date is the date of the provisional application, filed on August 30, 2012. However, my analysis would not change if the priority date were deemed to be the filing date of the PCT national phase application, August 28, 2013, or another date close to the filing date of the provisional application. In this declaration, I use the term “prior art” to refer to what was known and/or done before the priority date of the applicable patent.

THE '378 PATENT

10. Claims 1, 12 and 23 of the '378 Patent and their dependent claims (including claims 9, 11, 20, 22, 31 and 33) (the “Asserted Claims”) recite a method, apparatus and tangible machine readable storage medium for measuring exposure to media content across a variety of platforms in a manner that protects user privacy.

11. The Asserted Claims of the '378 Patent recite specific implementations of the invention disclosed in the patent. In particular, the claims recite: (1) sending of an encrypted identifier of a device or a device user to a corresponding database proprietor from an audience measurement entity (“AME”) (via a network communication from a server of the audience measurement entity); (2) receiving user information corresponding to the encrypted identifier from the database proprietor; (3) associating the user information with a media impression accessed via

the device or a search term collected at the device; and (4) other technical elements. *See* Asserted Claims.

12. The encryption of the device identifier and the use of the identifier to access a database to obtain user information (“the Encryption and Access Element”), as claimed in the Asserted Claims, was not well-understood, routine, or conventional in the prior art. Furthermore, the associating of user information with tracking information regarding instances of accessing data through the use of the above-element (“the Associating Element”), as claimed in the Asserted Claims, was not well-understood, routine, or conventional in the prior art is inventive and novel.

13. In practice, the Encryption and Access Element provides an approach to protect the privacy of individuals whose exposure to media content is being measured by encrypting unique identifiers and the subsequent resolution of such identifiers into anonymous pseudonyms. '378 Patent, 4:32-35. The Encryption and Access Element protects the privacy of the user of the mobile device because the device/user identifier is encrypted such that the AME cannot access it. *Id.*, 9:45-48. In practice, each database proprietor from which user information is sought is provided with an encryption key specific to that database proprietor. *Id.*, 9:54-59. In this manner, each database proprietor can only recover the device/user identifier that pertains to it. *Id.*, 9:59-62.

14. In the prior art, cookie-based techniques were used. Cookies exposed, or potentially exposed, users’ PII. *Id.*, 3:37-41, 3:53-4:3. Prior art cookie-based identifiers were limited to domains accessible to servers in the same domain and not to servers outside that domain. Moreover, while cookies can be an effective tool for devices using traditional web browsers (e.g., desktops), they are ineffective on mobile devices and smart TVs.

15. In practice, the Associating Element provides an approach to the associating of user information with tracking information regarding instances of accessing data through the use of the

Encryption and Access Element. The Associating Element is able to use multiple different types of device/user identifiers which increases the opportunities for collecting corresponding user information and is not tied to user information from a single source. *Id.*, 8:33-38.

16. As previously stated, this flexible design provides future proofing that allows the '378 Patent to be a long-term answer to obtaining user data. Prior art is contingent on singular concepts (e.g., cookies, code execution, etc.) that ultimately resulted in a need for a new solution due to the rise in mobile device popularity and their incompatibility with the methods and systems disclosed by prior art. It is because of such, that the '378 Patent is both innovative and highly practical in how it approached problems with user data analytics introduced by the popularity of mobile devices and smart TVs.

17. The disclosures of the '378 Patent also go beyond addressing the problem of obtaining user data from non-traditional browsers and addresses other problems as well. The methods and systems described by the patent allow for the access to user data by multiple network entities, which was not possible through the use of cookies. While other prior art (e.g., executing code on an end-user's device) could accomplish this task, such methods are also not effective outside of traditional browsing environments. This is also done in a way that protects the privacy and integrity of user data when delivering it to multiple servers through the use of security and encryption techniques. This as well is a novel concept in this context that was introduced by the '378 Patent which I further elaborate on below.

18. The provisional patent applications upon which the '378 Patent is based were filed in 2012. At that time, the combinations of elements recited in the asserted claims of the '378 Patent were not well-understood, routine, or conventional. See *id.*, 4:9-35.

19. The combination of the Encryption and Access Element and the Associating Element recited in the asserted claims of the '378 Patent solved technological problems experienced in prior art systems. See *id.*, 2:54-5:10. More particularly, the combination recites a method of protecting the privacy of individuals whose exposure to media content is being measured. See *id.*, 4:32-35. A key aspect of this approach is the encryption of user identity, and the use of the encrypted identifier by a database proprietor. See *id.*, 4:24-54. This combination is an inventive concept that was not well-understood, routine, or conventional at the time of the invention. See *id.*

20. Prior art in this space did not provide any guarantees regarding the security or privacy of user data. Cookies are a primitive method of storing user data in plaintext that did not have to be secured in any way, nor are there any guarantees that the data was transferred to a server via a secure channel, meaning a malicious entity could easily compromise user data. This could also affect the integrity of user data, as a malicious party could also manipulate the data in transit if it was not sent over a secure medium. Additionally, prior art methods involving code execution on a user's device to obtain data were problematic from a security and privacy perspective because they generally were not designed with attention to security in mind and because they were generally not concerned with protecting users' privacy.

21. In the past decade, data privacy and enhanced security features have received much needed attention and today there are many advanced security practices and privacy preserving protocols that provide users with data integrity and privacy guarantees. At the time of the '378 Patent's filing, however, common security and privacy practices were far inferior. The data privacy and integrity mechanisms described and claimed in the patent were novel for the time, especially

in the context of user data acquisition. This was an innovative feature for acquiring user data that was not being practiced by other prior art at the time.

CONCLUSION

22. I declare under penalty of perjury that the foregoing statements are true and correct to the best of my knowledge.

Dated: 2023 April 12

A handwritten signature in black ink, appearing to read "Paul D. Martin", is written over a horizontal line.

Paul D. Martin, Ph.D.